UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,424	04/10/2006	Yang Peng	CN 030035	3752

24737 7590 08/10/2009

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
08/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/575,424	PENG ET AL.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 17-32 are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/11/2009 has been entered.

Response to Arguments

2. Applicant's arguments filed 6/11/2009 have been fully considered but they are not persuasive.

Applicant argues that "authentication of the server does not by itself authenticate the content of the server" and "the server can be authenticated while the data stored on the authenticated server has been maliciously modified." The Examiner does not refute that, in some authentication systems, if a server is authenticated, the data may not be authentic. However, this does not have any bearing on the authentication of Uranaka, column 15, lines 57-67. Applicant's arguments appear to be made within the realm of authenticating the server wherein one will solely determine that the server is authentic through the authentication process. This corresponds to the server proving authenticity in a

separate step than sending of data (such as the downloaded content of the claims). One system that corresponds to such authentication may comprise certificate-based authentication, wherein the server proves that it can decrypt data that has been encrypted with its public key by a client. However, the authentication process performed in Uranaka unambiguously provides for authentication of the server and the data that is signed by the server in the same verification. As described in column 15, lines 57-67 of Uranaka, the server signs the double-encrypted AP-encrypting key with the server secret key. The client or player will then test the signature with the server public key. As one can see, the server first encrypts the data (the already twice-encrypted AP-encrypting key) with the server's secret key and sends this signed data to the client/player. The client then decrypts this data with the server's public key. This authenticates the server since the server is the only entity with access to the server secret key. It also authenticates the data, since the server is the only entity that could have encrypted the data, since it is the only entity with access to the sever secret key.

Taking a look at the well-known teachings of Bruce Schneier; section 2.6 of the book "Applied Cryptography" (Second Edition, 1996) provides for discussion regarding digital signatures. Within section 2.6, one can find the sub-section titled "Signing Documents with Public-Key Cryptography". This section describes the signing and verification/authentication that is performed by column 15, lines 57-67 of Uranaka. In this section, Alice (corresponding to the server of Uranaka) encrypts a document (AP-encrypting key of Uranaka) with her private key, thereby signing the document. This document is then sent to Bob

(corresponding to the player or client of Uranaka). Bob then decrypts the document using Alice's public key, thereby verifying the signature. This is how Uranaka works, as just described in the previous paragraph. Schneier then provides 5 beneficial characteristics that this procedure provides. Number 4 clearly states that "The signed document is unalterable; if there is any alteration to the document, the signature can no longer be verified with Alice's public key." Therefore, the data that is signed with the server public key in Uranaka must be authentic if the signature is verified. The pertinent portion of Schneier is included with this office action.

Claim Objections

3. Claims 17 and 32 are objected to because of the following informalities:

- Claim 17 refers to "the optical disk playing system", which has been construed as "the optical disk player" in order to provide proper antecedent basis.
- Claim 32 recites, in the last limitation, "playing the downloaded content stored on the optical disk in coordination with the downloaded content". This has been interpreted as "playing the media content stored on the optical disk in coordination with the downloaded content" as the downloaded content is not stored on the disk, but rather, the media content is.

Appropriate correction is required.

4. Claim 17 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The subject matter of claim 17 has already been conveyed in independent claim 20, from which claim 17 depends. In particular, claim 20 already states that the media content and a public key are stored on the optical disk and that the public key is used by the system to verify authenticity of the downloaded content before the stored media content is played in coordination with the downloaded content.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 17, 18, 20, 22-25, and 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Uranaka (U.S. Patent 6,470,085) in view of Tsumagari (U.S. Patent Application Publication 2004/0126095).

Regarding Claim 20,

Uranaka discloses an optical disk player, comprising:

An optical disk driver unit to read out media content and a public key stored on an optical disk (Column 6, lines 42-54; Column

7, lines 19-33; Column 8, lines 34-41; and Column 12, lines 12-15; showing the makeup of the DVD player including DVD DRIVER, applications stored on the optical disk (applications defined as music, movies, games, etc. in column 4, line 66 to column 5, line 1), server public key stored on the disk, and reading of such data from the disk);

A network interface to download content associated with the read out media content (Column 6, lines 42-58; Column 9, lines 30-46; and Column 9, line 61 to Column 10, line 20; showing the makeup of the DVD player including communication IF and interactions between the player and a server in order to download data associated with the content stored on the disk); and

A control system to verify the authenticity of the downloaded content using the public key read out from the optical disk before the read out media content is played (Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 15, lines 57-67; showing authentication of the server and the downloaded data, as described above in the response to arguments);

But does not explicitly disclose that the read out media content is played in coordination with the associated downloaded content.

Tsumagari, however, discloses that the read out media content is played in coordination with the associated downloaded

content (Paragraphs 43, 106, 116, 131, 156, and 174; showing downloading of ENAV contents from a server and playing of content from a DVD along with the ENAV contents). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the enhanced content system of Tsumagari into the content usage control system of Uranaka in order to allow the system to download enhanced data to supplement data stored on the optical disk, thereby ensuring that the player can always have the most up-to-date data without requiring a user to obtain a new disk.

Regarding Claim 25,

Claim 25 is a method claim that is broader than player claim 20 and is rejected for the same reasons.

Regarding Claim 22,

Uranaka as modified by Tsumagari discloses the player of claim 20, in addition, Tsumagari discloses that the downloaded content is an application program (Figure 10; and Paragraphs 143 and 167; ENAV contents comprising Java script for controlling reproduction of other ENAV contents, for example).

Regarding Claim 29,

Claim 29 is a method claim that is broader than player claim 22 and is rejected for the same reasons.

Regarding Claim 23,

Uranaka as modified by Tsumagari discloses the player of claim 22, in addition, Tsumagari discloses that the application program is a JAVA language application program (Figure 10; and Paragraphs 143 and 167, as just described).

Regarding Claim 30,

Claim 30 is a method claim that is broader than player claim 23 and is rejected for the same reasons.

Regarding Claim 24,

Uranaka as modified by Tsumagari discloses the player of claim 20, in addition, Uranaka discloses that the control system verifies the authenticity of the downloaded content by performing asymmetric cryptography using the public key stored on the optical disk and corresponding to a private key used to encrypt the downloaded content (Column 15, lines 57-67).

Regarding Claim 31,

Claim 31 is a method claim that is broader than player claim 24 and is rejected for the same reasons.

Regarding Claim 17,

Uranaka as modified by Tsumagari discloses the player of claim 20, in addition, Uranaka discloses that the optical disk comprises digital information stored there, the stored digital information comprising:

Stored media content that is played in coordination with downloadable content associated with the stored media content (Figure 2; and Column 4, line 66 to Column 5, line 42; as described above with respect to playing "in coordination" in the combination); and

A public key which is used by the optical disk player to verify the authenticity of the downloadable content before the stored media content is played in coordination with the associated downloadable content (Figures 2 and 4; Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 15, lines 57-67; as described above).

Regarding Claim 18,

Uranaka as modified by Tsumagari discloses the player of claim 17, in addition, Uranaka discloses that the public key is stored in a BCA zone of the optical disk (Figures 2 and 4; Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 8, lines 34-41).

Regarding Claim 32,

Uranaka as modified by Tsumagari discloses the method of claim 25, in addition, Uranaka discloses that the optical disk comprises digital information stored thereon, the stored digital information comprising:

Server information that is used by the optical disk playing system to download content for playing the optical disk (Figures 2 and 4; Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 15, lines 57-67); and

A public key that is used by the optical disk playing system to verify the authenticity of downloaded content before playing the media content stored on the optical disk in coordination with the downloaded content (Figures 2 and 4; Column 5, liens 2—42; Column 5, line 58 to Column 6, line 5; and Column 15, lines 57-67); and

Tsumagari discloses that the server information comprises a network address (Paragraph 39).

6. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Uranaka in view of Tsumagari, further in view of Ryan (U.S. Patent 5,754,648).

Uranaka as modified by Tsumagari does not explicitly disclose that the public key is stored in a media content zone of the optical disk.

Ryan, however, discloses that the public key is stored in a media content zone of the optical disk (Column 3, lines 47-67; and Column 8, lines 31-37). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the media security and tracking system of Ryan into the content usage control system of Uranaka as modified by Tsumagari in order to allow the system to provide

additional authentication and authorization steps such that a device can ensure that both the disk and device are authentic and authorized for use with each other by using data stored on the optical disk itself and data stored on a magnetic track attached to the disk, thus decreasing the chance of unauthorized use thereof, and/or to provide the ability to track use of the media.

7. Claims 21 and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Uranaka in view of Tsumagari, further in view of Collins (U.S. Patent Application Publication 2002/0073316).

Regarding Claim 21,

Uranaka as modified by Tsumagari does not explicitly disclose that the control system detects whether the downloaded content is integral before verification, wherein the verification will not be executed if the downloaded content is detected to not be integral.

Collins, however, discloses that the control system detects whether the downloaded content is integral before verification, wherein the verification will not be executed if the downloaded content is detected to not be integral (Paragraphs 73-77; detecting whether the downloaded content is "integral" may comprise either, or both, verification of the program packet format and/or verification of the checksum, each of which must succeed before signature

verification is performed). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content authentication and access control system of Collins into the content usage control system of Uranaka as modified by Tsumagari in order to allow the system to detect when errors in the data have occurred, such that data with errors will not be allowed to be processed and only correct data will be processed, and/or to ensure that the data is authentic before allowing access to proceed, thereby increasing security of the system by ensuring both integrity and authenticity of the content.

Regarding Claim 26,

Claim 26 is a method claim that is broader than player claim 21 and is rejected for the same reasons.

Regarding Claim 27,

Uranaka as modified by Tsumagari discloses that authentication of the downloaded content is performed prior to playing the read out media content in coordination with downloaded content (Uranaka, Column 15, lines 57-67, for example, as well as the discussion above with respect to playing in coordination), but does not explicitly disclose that the downloaded content will not be used if the downloaded content is not authenticated.

Collins, however, discloses that the downloaded content will not be used if the downloaded content is not authenticated

(Paragraphs 73-78; showing that if any of the verification steps, including authentication of the digital signature, fail, the process will abort and the data will not be used). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content authentication and access control system of Collins into the content usage control system of Uranaka as modified by Tsumagari in order to allow the system to detect when errors in the data have occurred, such that data with errors will not be allowed to be processed and only correct data will be processed, and/or to ensure that the data is authentic before allowing access to proceed, thereby increasing security of the system by ensuring both integrity and authenticity of the content.

Regarding Claim 28,

Uranaka as modified by Tsumagari and Collins discloses the method of claim 27, in addition, Uranaka discloses that the coordination between the read out media and downloaded content will be established if the downloaded content is authenticated (Column 15, lines 57-67); and Collins discloses allowing use of downloaded content if the downloaded content is authenticated (Paragraphs 73-77).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437